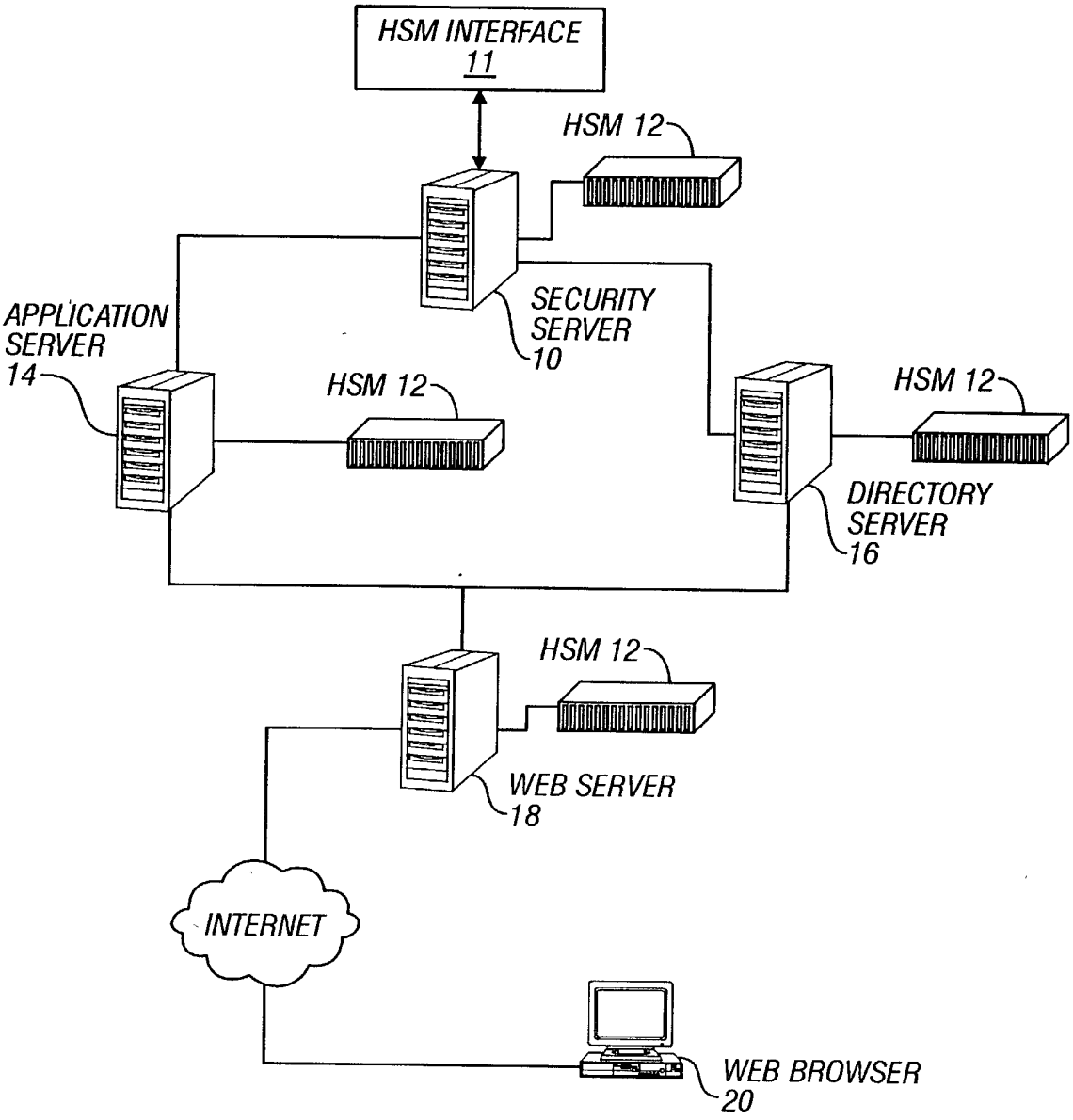

FIG. 1
(Prior Art)

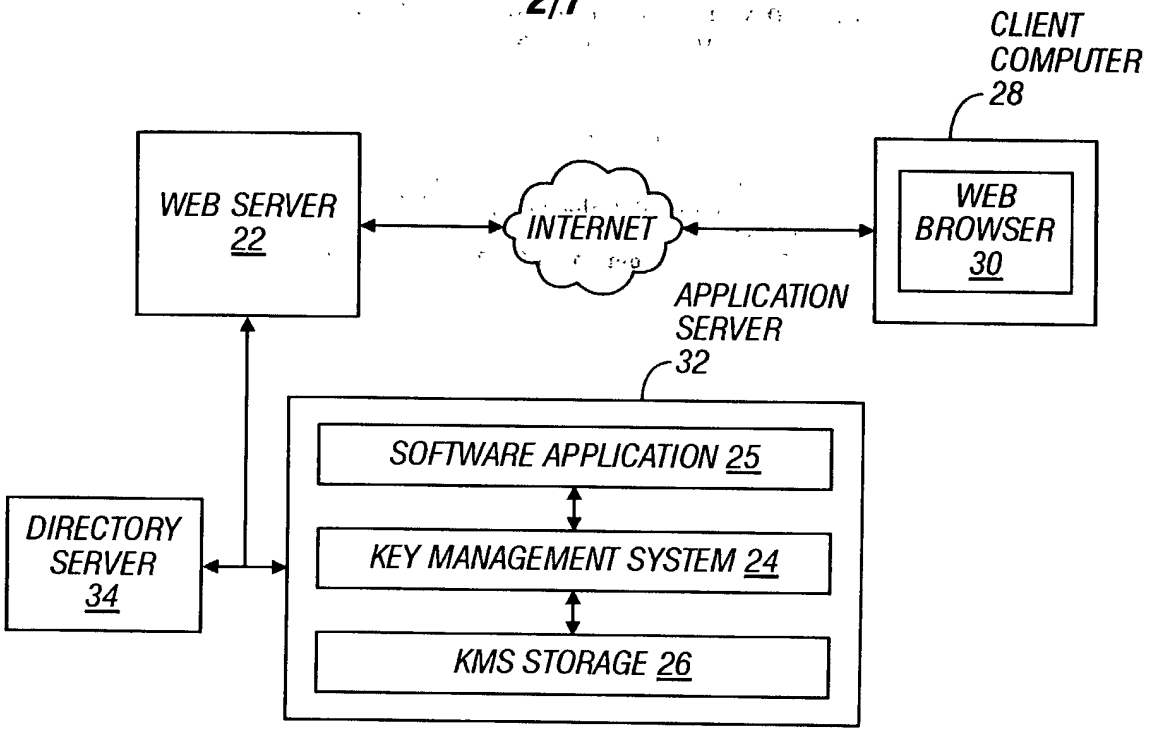
CLIENT COMPUTER 28
WEB SERVER 22
INTERNET
WEB BROWSER 30
APPLICATION SERVER 32
SOFTWARE APPLICATION 25
KEY MANAGEMENT SYSTEM 24
KMS STORAGE 26
DIRECTORY SERVER 34

FIG. 2

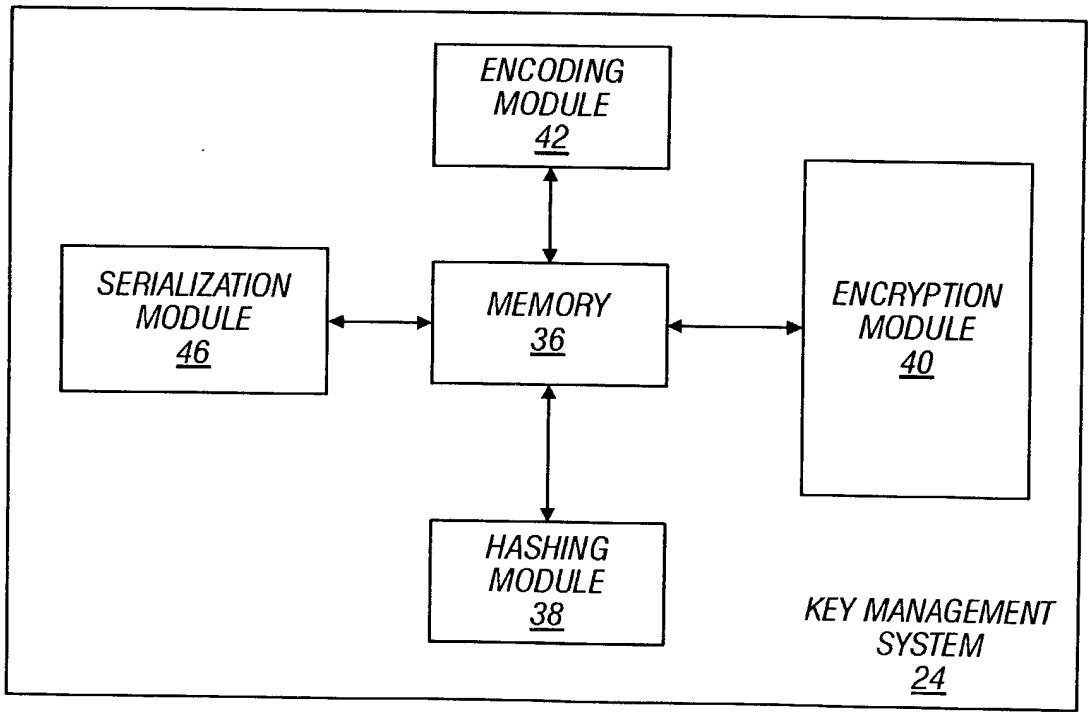
ENCODING MODULE 42
SERIALIZATION MODULE 46
MEMORY 36
ENCRYPTION MODULE 40
HASHING MODULE 38
KEY MANAGEMENT SYSTEM 24

FIG. 3

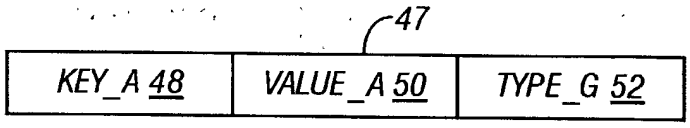

FIG. 4

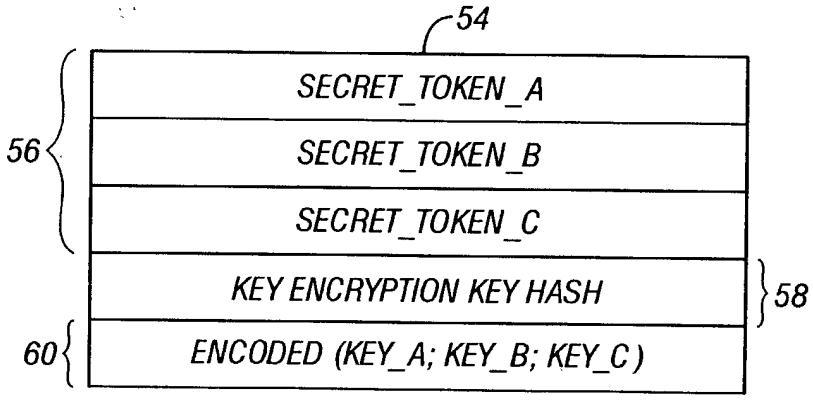

FIG. 5

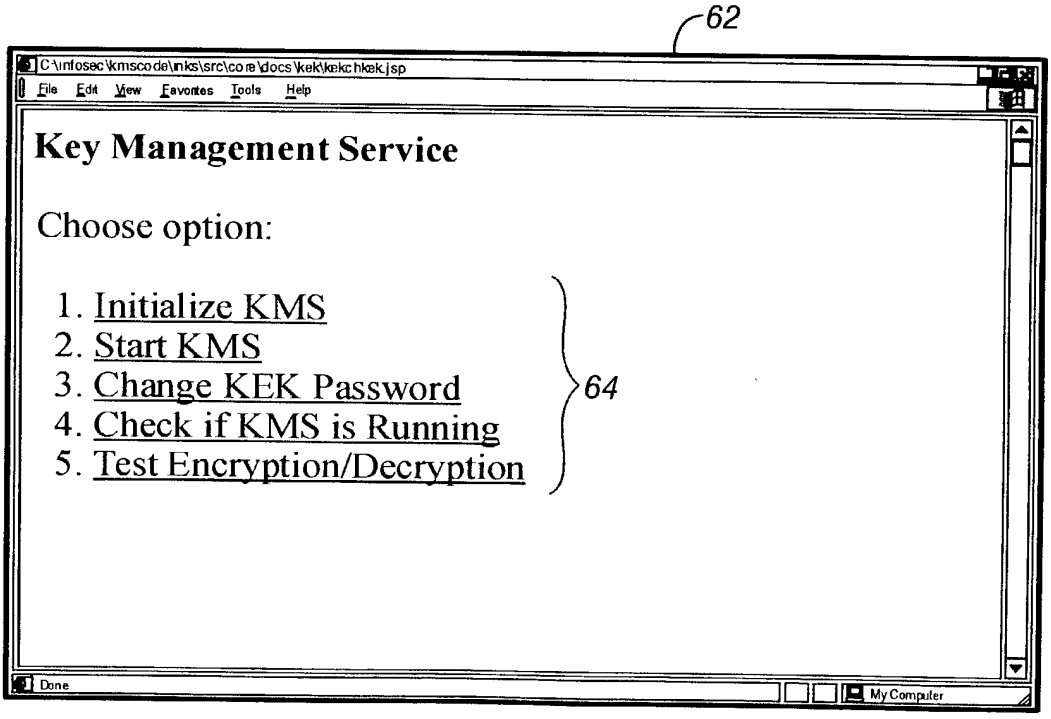

FIG. 6

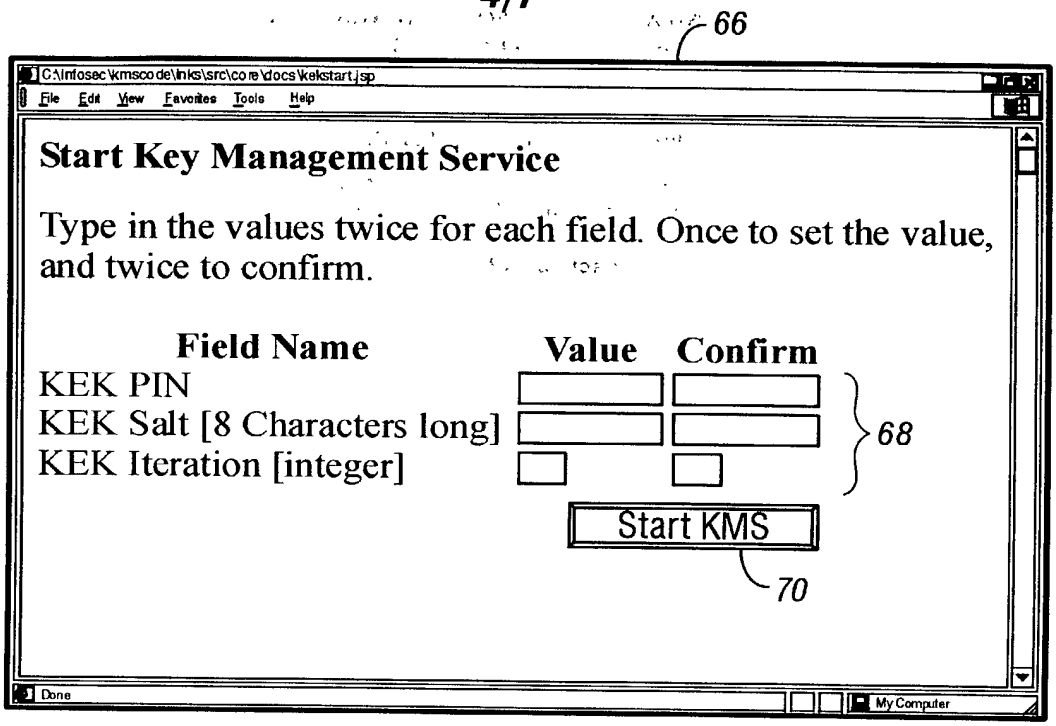
66
C:\infosec\kmscode\inks\src\core\docs\kekstart.jsp
File Edit View Favorites Tools Help
Start Key Management Service
Type in the values twice for each field. Once to set the value, and twice to confirm.
Field Name
Value
Confirm
KEK PIN
KEK Salt [8 Characters long]
KEK Iteration [integer]
68
Start KMS
70
Done
My Computer

FIG. 7

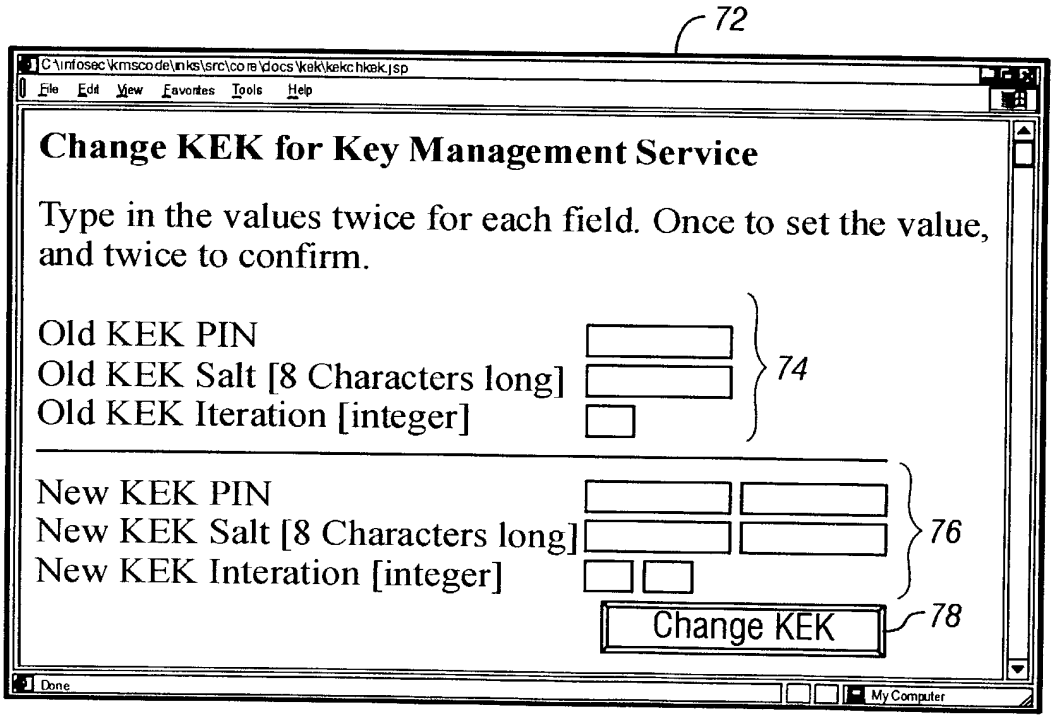
72
C:\infosec\kmscode\inks\src\core\docs\kek\kekchkek.jsp
File Edit View Favorites Tools Help
Change KEK for Key Management Service
Type in the values twice for each field. Once to set the value, and twice to confirm.
Old KEK PIN
Old KEK Salt [8 Characters long]
Old KEK Iteration [integer]
74
New KEK PIN
New KEK Salt [8 Characters long]
New KEK Interation [integer]
76
Change KEK
78
Done
My Computer

FIG. 8

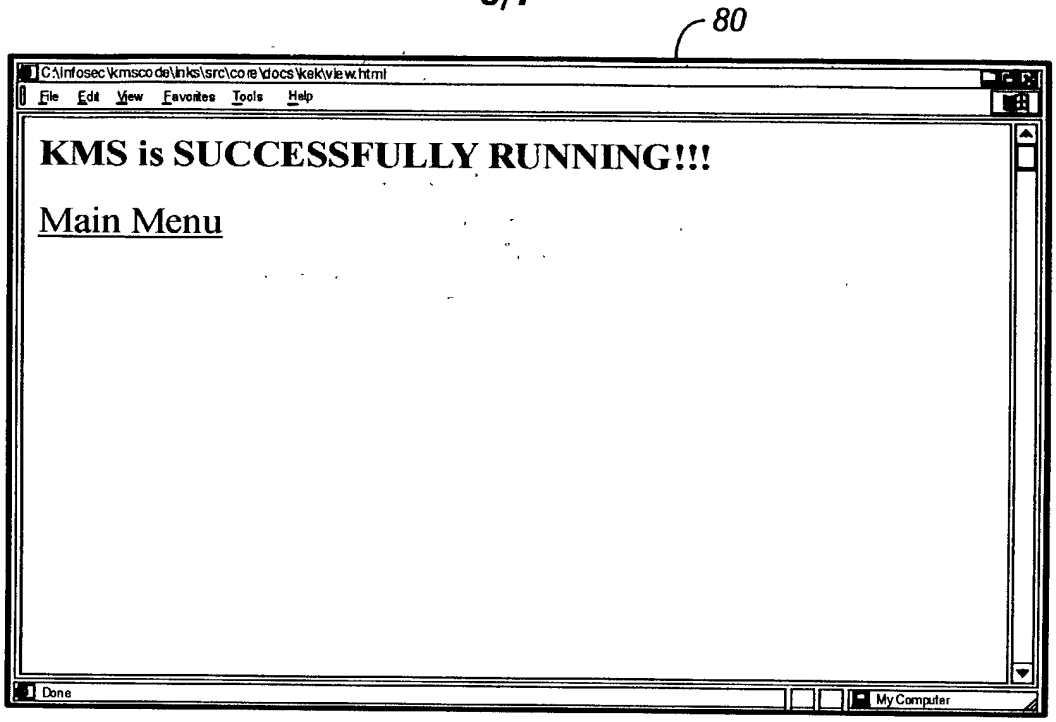
80
C:\infosec\kmscode\inks\src\core\docs\kek\view.html
File Edit View Favorites Tools Help
KMS is SUCCESSFULLY RUNNING!!!
Main Menu
Done
My Computer

FIG. 9

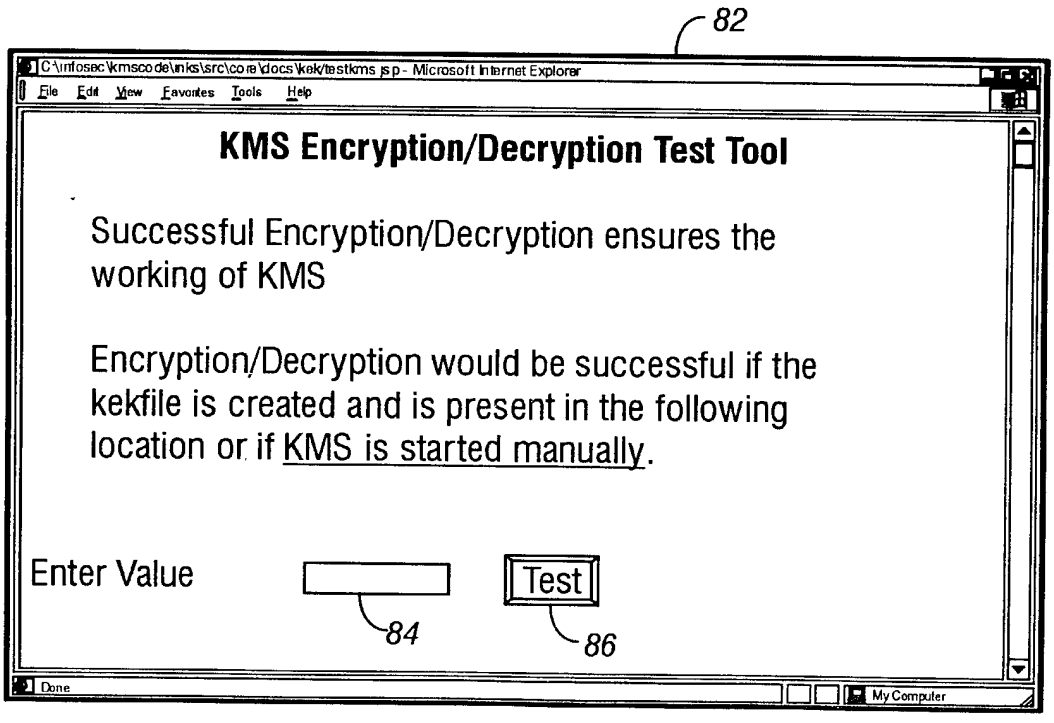
82
C:\infosec\kmscode\inks\src\core\docs\kek\testkms.jsp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
KMS Encryption/Decryption Test Tool
Successful Encryption/Decryption ensures the working of KMS
Encryption/Decryption would be successful if the kekfile is created and is present in the following location or if KMS is started manually.
Enter Value
84
Test
86
Done
My Computer

FIG. 10

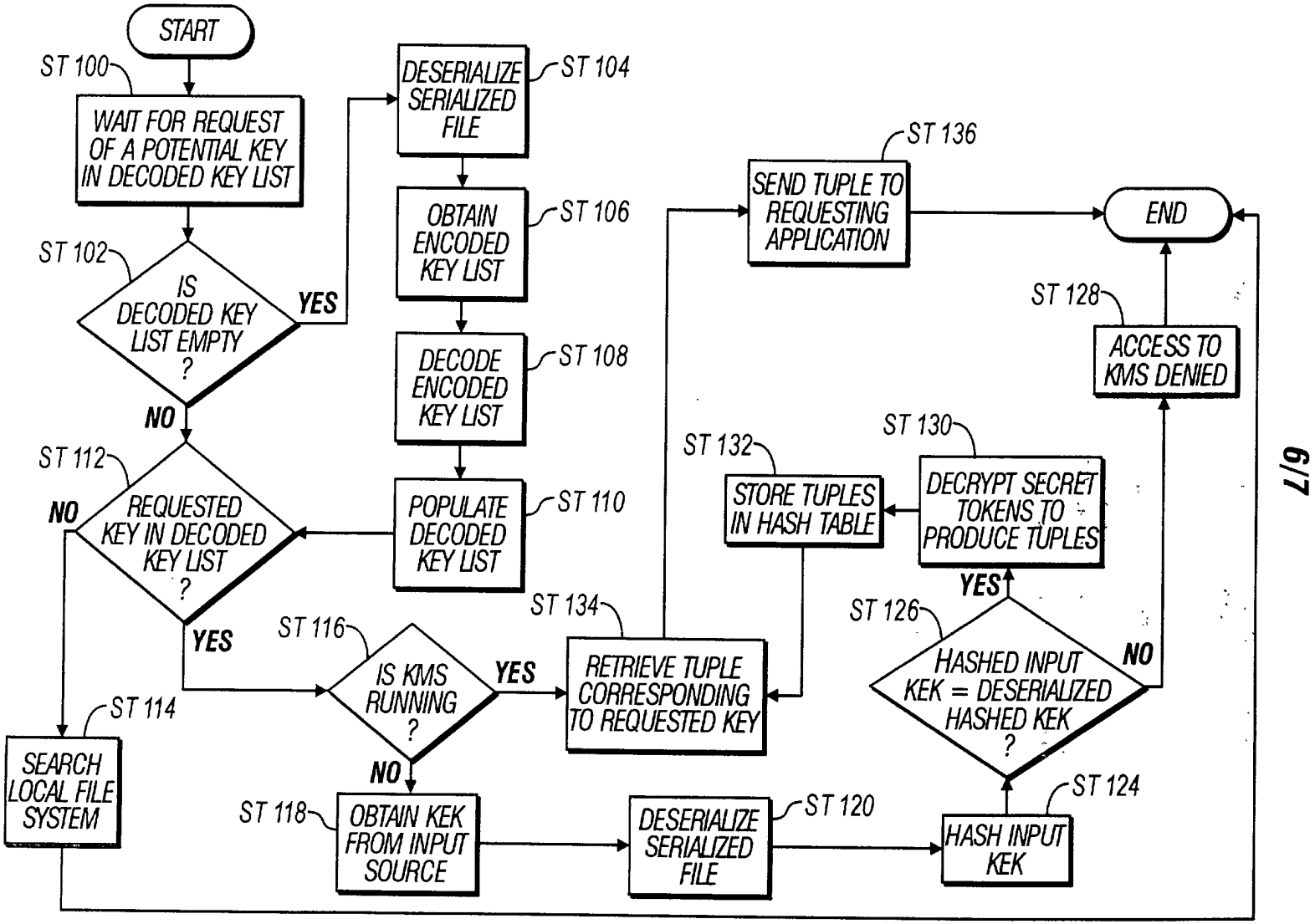

FIG. 11

4008275B - 05220802

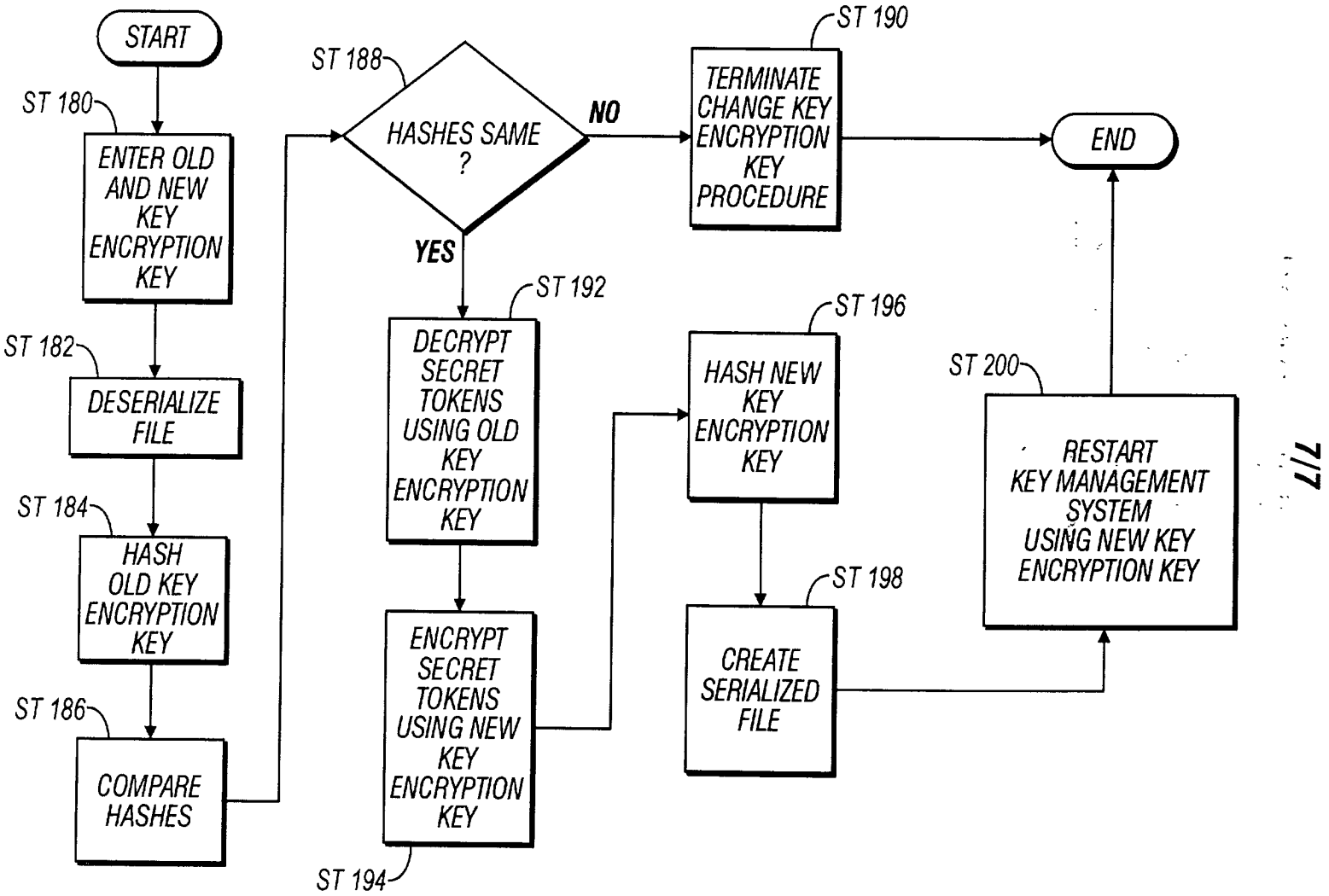
START
ST 180
ENTER OLD AND NEW KEY ENCRYPTION KEY
ST 182
DESERIALIZE FILE
ST 184
HASH OLD KEY ENCRYPTION KEY
ST 186
COMPARE HASHES
ST 188
HASHES SAME ?
NO
YES
ST 190
TERMINATE CHANGE KEY ENCRYPTION KEY PROCEDURE
END
ST 192
DECRYPT SECRET TOKENS USING OLD KEY ENCRYPTION KEY
ST 194
ENCRYPT SECRET TOKENS USING NEW KEY ENCRYPTION KEY
ST 196
HASH NEW KEY ENCRYPTION KEY
ST 198
CREATE SERIALIZED FILE
ST 200
RESTART KEY MANAGEMENT SYSTEM USING NEW KEY ENCRYPTION KEY

FIG. 12